PATENT
29250-002013/US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPELLANTS:	Sarvar PATEL et al.	CONF. NO.:	5912
APPL'N NO.:	10/786,454	GROUP:	2439
FILED:	February 26, 2004	EXAMINER:	Roderick Tolentino
FOR:	METHOD OF GENERATING A CRYPTOSYNC		

APPELLANTS' BRIEF ON APPEAL UNDER 37 C.F.R. § 41.37

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314
Mail Stop Appeal Briefs - Patents

November 3, 2011

Sir/Madam:

In response to the non-final Office Action issued on June 3, 2011, Appellants hereby submit their Brief on Appeal in accordance with 37 C.F.R. § 41.37. The due date of the Appeal Brief is extended by two (2) months to November 3, 2011 by the attached Petition for Extension of Time. The government fees for filing a Notice of Appeal ($540) and filing a brief in support of an appeal ($540) were previously paid and are not required to be paid again at this time. However, the fees have increased since the previous Notice of Appeal and Appeal Brief were filed, and therefore Appellants pay the difference at this time (an additional $160).

Adjustment date: 11/04/2011 AWONDAF1
03/22/2011 INTEFSW 00006704 000750 10786454
02 FC:1402 540.00 CR

11/04/2011 AWONDAF1 00000020 000750 10786454
01 FC:1402 540.00 DA 80.00 OP

I. REAL PARTY IN INTEREST.

The real party in interest is Alcatel-Lucent.

II. RELATED APPEALS AND INTERFERENCES.

No related appeals or interferences are known.

III. STATUS OF CLAIMS.

Claims 1-24 are currently pending in the present application. Claims 1 and 24 are independent claims.

Claim 5 stands rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 4, 6, 7, 11, and 12 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Publication 2005/0086468 to Meandzija et al. ("Meandzija") in view of U.S. Patent Publication 2004/0078334 to Malcolm et al. ("Malcolm").

Claims 2 and 3 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Meandzija in view of Malcolm in further view of U.S. Patent Publication 2005/0172116 to Burch et al. ("Burch").

Claim 5 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Meandzija in view of Malcolm in further view of U.S. Patent Publication 2005/0177715 to Somin et al. ("Somin").

Claims 8-10 and 13-23 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Meandzija in view of Malcolm in further view of U.S. Patent 6,980,658 to Rezaiifar et al. ("Rezaiifar").

Claim 24 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Meandzija in view of Malcolm and Burch.

Claims 1-24 are being appealed.

IV. STATUS OF AMENDMENTS.

An Amendment under 37 CFR 1.111 was filed on March 1, 2010, with a further Supplemental Amendment filed on April 8, 2010. A Final Office Action was mailed July 1, 2010. A Notice of Appeal and Pre-Appeal Brief Request for Review were filed on December 1, 2010, and an Appeal Brief was filed on March 21, 2011. A non-final Office Action was issued on June 3, 2011 reopening prosecution.

V. SUMMARY OF CLAIMED SUBJECT MATTER.

A. CONCISE EXPLANATION OF THE SUBJECT MATTER SET FORTH IN EACH CLAIM ARGUED SEPARATELY.

1. A GENERAL DISCUSSION OF THE SUBJECT MATTER DESCRIBED IN THE SPECIFICATION TO ASSIST THE BOARD IN UNDERSTANDING EXAMPLE EMBODIMENTS DESCRIBED IN THE PRESENT APPLICATION.

Encryption is used in numerous fields including wireless networks and internet communication. Some encryption algorithms such as DES, AES, etc. involve the use of a key which is a bit sequence used in the encryption algorithm

to generate the ciphertext. The encryption key is known at both the send and receive sides of the communication, and at the receive side is used to decrypt the ciphertext into the plaintext.

For example encryption in the wireless communication environment may involve encrypting frames of information sent between a base station and a mobile station. With some encryption schemes, if the same information is encrypted and sent during two different frames, the same ciphertext is produced. This ciphertext can be intercepted by a malicious entity and used by the malicious entity to impersonate another user in what is referred to as a replay attack.

One way to prevent replay attacks is to use cryptosyncs. Cryptosyncs are used in conjunction with encryption and decryption keys. Cryptosyncs have values which change over time so that cipher text generated by an encryption operation changes even when the plain text, which is encrypted, does not.[1]

Example embodiments provide methods for generating cryptosyncs for use in communications between, for example, two devices.

In wireless communication, mobile stations communicate with base stations over the air. This communication may be encrypted. In CDMA2000, for example, long lived keys such as a cipher key (CK) and an integrity key (IK) associated with a mobile station that are used in the encryption processes and messaging integrity protection processes, respectively. CDMA2000 also provides for, relatively speaking, a long lived cryptosync (e.g., TX_EXT_SSEQ and RX_EXT_SSEQ in CDMA2000). The long-lived cryptosync (LLCS) is used to encrypt and decrypt messages (e.g., signaling messages) between the base station

[1] Spec. at p. 1-2.

and mobile station, to verify message integrity, or both. After each use, the LLCS is incremented to prevent susceptibility to replay attacks. Initially, upon need or request, the LLCS may be derived using any well-known authentication protocol such as set forth in CDMA2000.[2]

One protocol for data communication between the base station and mobile station, for example, is referred to as the radio link protocol (RLP). To establish an RLP communication, a communication channel between the mobile station and base station is established in a well-known manner such as through message integrity using the LLCS. When the RLP communication ends, the communication channel is torn down. The time during which the communication channel existed for communication of information (e.g., voice, data, etc.) is referred to generally as the communication session. During a communication session, several frames, as defined by the RLP may be communicated. Each frame is encrypted using what will be referred to hereafter as a short-lived cryptosync (SLCS). The SLCS is short lived in comparison to the LLCS in that the life of the SLCS is limited to the duration of the communication session. A value for the SLCS is newly derived for each communication session.[3]

---

[2] Id. at p. 4-5.
[3] Id. at p. 5-6.

2. AN EXPLANATION OF THE SUBJECT MATTER SET FORTH IN EACH CLAIM ARGUED SEPARATELY REFERRING TO THE SPECIFICATION AND/OR THE DRAWINGS BY REFERENCE CHARACTERS IN ACCORDANCE WITH 37 C.F.R. § 41.37(c)(1)(v).

I. CLAIM 1.

Claim 1 recites "A method of generating a cryptosync for a communication session between two communication devices, comprising: deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync". This limitation is supported by at least paragraph [0018][4] of Appellants' specification, herein after referred to as 'the specification', which explains that a first cryptosync, an SLCS, is derived using a portion or the entirety of a second cryptosync, an LLCS.

Claim 1 also recites "the first cryptosync having a life limited to the communication session, the communication session being defined as a period of time a channel for communication exists between the two communication devices, the second cryptosync having a life extending over multiple communication sessions." These limitations are supported by at least by at least paragraph [0014][5] of the specification which explains that the time period during which a communication channel exists for communication of information is referred to as a communication session; paragraph [0015][6] of the specification, which explains that the SLCS has a life limited to the duration of a communications session; and

[4] Id. at p. 7, l. 17 –p. 8, l. 4.
[5] Id. at p. 5, l. 15 – p. 6, l. 6.
[6] Id. at p. 6, l. 7 –14.

paragraph [0016][7] of the specification, which explains that LLCS has a life that extends over multiple communications sessions.

II. CLAIMS 2-4.

Claim 2 depends from claim 1 and recites "wherein the second cryptosync is used for message encryption by at least one of the two devices". Claims 3 and 4 depend from claims 2 and 1, respectively, and recite "wherein the second cryptosync is used for verifying message integrity by at least one of the two devices". These limitations are supported by at least paragraph [0013][8] of the specification which explains that the LLCS is used to encrypt and decrypt messages between a base station and a mobile and/or to verify message integrity.

III. CLAIM 5

Claims 5 depends from claim 1 and recites "wherein the second cryptosync changes between communication sessions". These limitations are supported by at least paragraph [0017][9] of the specification which explains that the LLCS may be incremented between communications sessions.

IV. CLAIM 6

Claim 6 depends from claim 1 and recites "wherein the deriving step derives the first cryptosync as at least a portion of the second cryptosync". This

[7] Id. at p. 6, l. 15 -p. 7, l. 6.
[8] Id. at p. 4, l. 17 -p. 5, l. 14.
[9] Id. at p. 7, l. 7 -16.

limitation is supported by paragraph [0018][10] of the specification which explains that the SLCS is derived using a portion or the entirety of the LLCS.

V. CLAIM 7

Claim 7 depends from claim 6 and recites "wherein the deriving step derives the first cryptosync as at least a portion of the second cryptosync and a fixed bit sequence". This limitation is supported by at least Appellants' FIG. 1 and paragraph [0018][11] of the specification which explain that an SLCS may have, for example, 64 bits, 32 bits of which are the LLCS and 32 bits of which are a fixed bit stream.

VI. CLAIM 8

Claim 8 depends from claim 7 and recites "wherein the deriving step derives most significant bits of the first cryptosync as the portion of the second cryptosync and derives least significant bits of the first cryptosync as the fixed bit sequence". This limitation is supported by at least Appellants' FIG. 1 and paragraph [0018][12] of the specification which explain that an SLCS may have, for example, 64 bits of which the 32 most significant bits are the LLCS and the 32 least significant bits are a fixed bit stream.

VII. CLAIM 9

Claim 9 depends from claim 8 and recites "wherein the fixed bit sequence is a string of 0s". This limitation is supported by at least Appellants' FIG. 1 which

---

[10] Id. at p. 7, l. 17 –p. 8, l. 4.
[11] Id.
[12] Id.

illustrates the fixed bit sequence occupying the least significant 32 bits of the SLCS being 0s.

VIII. CLAIM 10

Claim 10 depends from claim 8 and recites "wherein the deriving step derives a 32 most significant bits of the first cryptosync as the second cryptosync and derives a 32 least significant bits of the first cryptosync as a string of 0s". This limitation is supported by at least Appellants' FIG. 1 which illustrates an SLCS having 64 bits of which the 32 most significant bits are the LLCS and the 32 least significant bits are 0s.

IX. CLAIM 11

Claim 11 depends from claim 6 and recites "wherein the deriving step derives a portion of the first cryptosync as the second cryptosync". These limitations are supported by at least Appellants' FIG. 1 which illustrates an SLCS having 64 bits of which the 32 most significant bits are the entire 32 bits of the LLCS. Accordingly, a portion of the first cryptosync is the second cryptosync.

X. CLAIM 12

Claim 12 depends from claim 11 and recites "wherein the deriving step derives a first portion of the first cryptosync as the second cryptosync and derives a second portion of the first cryptosync as a fixed bit sequence". This limitation is supported by at least Appellants' FIG. 1 which illustrates an SLCS having 64 bits

of which the 32 most significant bits are the LLCS and the 32 least significant bits are a fixed bit sequence, 0s.

XI. CLAIM 13

Claim 13 depends from claim 12 and recites "wherein the fixed bit sequence is a string of 0s". This limitation is supported by at least Appellants' FIG. 1 which illustrates an SLCS having 64 bits of which the 32 most significant bits are the LLCS and the 32 least significant bits are a string of 0s.

XII. CLAIMS 14-15

Claim 14 depends from claim 1 and recites "wherein the deriving step comprises: performing a pseudo-random function on the second cryptosync; and generating the first cryptosync from output of the pseudo-random function." Claim 15 depends from claim 14 and recites "wherein the generating step generates the first cryptosync as the output of the pseudo-random function". These limitations are supported by at least paragraph [0020][13] of Appellants' specification which discuss applying a pseudo random function to the LLCS and using the resulting pseudo-random number as the SLCS.

XIII. CLAIMS 16-17

Claim 16 depends from claim 1 and recites "wherein the deriving step is performed at a base station". Claim 17 depends from claim 1 and recites "wherein

[13] Id. at p. 8, l. 10-16.

the deriving step is performed at a mobile station". These limitations are supported by at least paragraph [0022][14] of Appellants' specification which explains that because the LLCS is know at both the mobile station and the bases station, the same SLCS can be derived at both. Further, the same SLCS can be used to encrypt sent information at either the mobile or base station, and to decrypt received data at either the mobile or bases station.

XIV. CLAIMS 18-20

Claim 18 depends from claim 1 and recites "further comprising: encrypting a frame of information to send from the at least one of the two devices using the first cryptosync." Claim 19 depends from claim 18, and recites "wherein the frame of information is a radio link protocol, RLP, frame". Claim 20 depends from claim 18 and recites "further comprising: incrementing the first cryptosync after the encrypting step." These limitations are supported by at least paragraph [0015][15] of Appellants specification which discusses encrypting RLP frames using the SLCS; and paragraph [0022][16] of the specification which discusses encrypting a frame of information at the send side for either the mobile or the base station using the SLCS, and incrementing the SLCS for use in encrypting the next frame.

[14] Id. at p. 8, l. 21-p. 9, l. 9.
[15] Id. at p. 6, l. 7 -14.
[16] Id. at p. 8, l. 21-p. 9, l. 9.

XV. CLAIMS 21-23

Claim 21 depends from claim 1 and recites "[t]he method of claim 1, further comprising: decrypting a frame of information received at the at least one of the two devices using the first cryptosync." Claim 22 depends from claim 21 and recites "wherein the frame of information is a radio link protocol, RLP, frame". Claim 23 depends from claim 21 and recites "further comprising: incrementing the first cryptosync after the decrypting step." These limitations are supported by at least paragraph [0015][17] of the specification which discusses encrypting RLP frames using the SLCS; and paragraph [0022][18] of the specification which discusses encrypting a frame of information at the send side for either the mobile or the base station using the SLCS, decrypting that same frame of information at the receiving side for either the mobile or the base station using the SLCS, and incrementing the SLCS for use in decrypting the next frame.

XVI. CLAIM 24

Claim 24 recites "deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync used to encrypt further communication between the two devices". This limitation is supported by at least paragraph [0018][19] of the specification, which explains that a first cryptosync, the SLCS, is derived using portion or the entirety of the second cryptosync, the LLCS.

---

[17] Id. at p. 6, l. 7 -14.
[18] Id. at p. 8, l. 21-p. 9, l. 9.
[19] Id. at p. 7, l. 17 -p. 8, l. 4.

Claim 24 also recites "the first cryptosync having a life limited to the communication session, the communication session being defined as a period of time a channel for communication exists between the two communication devices, the second cryptosync having a life extending over multiple communication sessions". These limitations are supported by at least paragraph [0014][20] of the specification which explains that the time period during which a communication channel exists for communication of information is referred to as a communication session; paragraph [0015][21] of the specification, which explains that the SLCS has a life limited to the duration of a communications session; and paragraph [0016][22] of the specification, which explains that LLCS has a life that extends over multiple communications sessions.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL.

A. APPELLANTS SEEK THE BOARD'S REVIEW OF THE REJECTION OF CLAIM 5 UNDER 35 U.S.C. §112, SECOND PARAGRAPH, AS BEING INDEFINITE FOR FAILING TO PARTICULARLY POINT OUT AND DISTINCTLY CLAIM THE SUBJECT MATTER WHICH APPLICANT REGARDS AS THE INVENTION.

B. APPELLANTS SEEK THE BOARD'S REVIEW OF THE REJECTION OF CLAIMS 1, 4, 6, 7, 11, AND 12 UNDER 35 U.S.C. §103(A) AS BEING UNPATENTABLE OVER U.S. PATENT PUBLICATION 2005/0086468 TO MEANDZIJA ET AL. ("MEANDZIJA") IN VIEW OF U.S. PATENT PUBLICATION 2004/0078334 TO MALCOLM ET AL. ("MALCOLM").

C. APPELLANTS SEEK THE BOARD'S REVIEW OF THE REJECTION OF CLAIMS 2 AND 3 UNDER 35 U.S.C. §103(A) AS BEING UNPATENTABLE OVER MEANDZIJA IN VIEW OF MALCOLM IN FURTHER VIEW OF U.S. PATENT PUBLICATION 2005/0172116 TO BURCH ET AL. ("BURCH").

D. APPELLANTS SEEK THE BOARD'S REVIEW OF THE REJECTION OF CLAIM 5 UNDER 35 U.S.C. §103(A) AS BEING UNPATENTABLE OVER MEANDZIJA IN

[20] Id. at p. 5, l. 15 –p. 6, l. 6.
[21] Id. at p. 6, l. 7 –17.
[22] Id. at p. 6, l. 15 –p. 7, l. 6.

VIEW OF MALCOLM IN FURTHER VIEW OF U.S. PATENT PUBLICATION 2005/0177715 TO SOMIN ET AL. ("SOMIN").

E. APPELLANTS SEEK THE BOARD'S REVIEW OF THE REJECTION OF CLAIMS 8-10 AND 13-23 UNDER 35 U.S.C. §103(A) AS BEING UNPATENTABLE OVER MEANDZIJA IN VIEW OF MALCOLM IN FURTHER VIEW OF U.S. PATENT 6,980,658 TO REZAIIFAR ET AL. ("REZAIIFAR").

F. APPELLANTS SEEK THE BOARD'S REVIEW OF THE REJECTION OF CLAIM 24 UNDER 35 U.S.C. §103(A) AS BEING UNPATENTABLE OVER MEANDZIJA IN VIEW OF MALCOLM AND BURCH.

Claims 1-24 are being appealed.

VII. ARGUMENT.

PRINCIPLES OF LAW

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention (35 U.S.C. §112, second paragraph). In reviewing a claim for compliance with 35 U.S.C. 112, second paragraph, the examiner must consider the claim as a whole to determine whether the claim apprises one of ordinary skill in the art of its scope and, therefore, serves the notice function required by 35 U.S.C. 112, second paragraph, by providing clear warning to others as to what constitutes infringement of the patent.[23] Further, the following has been held: "[t]he requirement to 'distinctly' claim means that the claim must have a meaning discernible to one of ordinary skill in the art when construed according to correct principles. Only when a claim remains insolubly ambiguous

[23] *Solomon v. Kimberly-Clark Corp.*, 216 F.3d 1372, 1379, 55 USPQ2d 1279, 1283 (Fed. Cir. 2000); *In re Larsen*, No. 01-1092 (Fed. Cir. May 9, 2001).

without a discernible meaning after all reasonable attempts at construction must a court declare it indefinite".[24]

Under 35 U.S.C. §103(a) a patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made (35 U.S.C. §103(a)).

The Examiner bears the initial burden of presenting a *prima facie* case of obviousness in rejecting claims under 35 U.S.C. §103.[25] In rejecting claims under 35 U.S.C. §103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness.[26] In so doing, the Examiner must make the factual determinations set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17, 148 USPQ 459, 467 (1966), *viz.*, (1) the scope and content of the prior art; (2) the differences between the prior art and the claims at issue; and (3) the level of ordinary skill in the art. Furthermore, "'there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness'...[H]owever, the analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the

---

[24] *Metabolite Labs., Inc. v. Lab. Corp. of Am. Holdings*, 370 F.3d 1354, 1366, 71 USPQ2d 1081, 1089 (Fed. Cir. 2004).
[25] *In re Rijckaert*, 9 F.3d 1531, 1532, 28 USPQ2d 1955, 1956 (Fed. Cir. 1993).
[26] *In re Fine*, 837 F.2d 1071, 1073, 5 USPQ2d 1956, 1958 (Fed. Cir. 1988).

would employ."[27] Obviousness is then determined on the basis of the evidence as a whole and the relative persuasiveness of the arguments.[28]

A. APPELLANTS SEEK THE BOARD'S REVIEW OF THE REJECTION OF CLAIM 5 UNDER 35 U.S.C. §112, SECOND PARAGRAPH AS BEING INDEFINITE.

ARGUMENTS

In rejecting claim 5, the June 3, 2011 Office Action (hereinafter, "the Office Action") asserts claim 5 is indefinite. Appellants respectfully disagree with this assertion.

Claim 5 recites "wherein the second cryptosync changes between communication sessions". The Office Action notes, on page 3, claim 1 requires the second cryptosync to have a life which extends over multiple communication sessions. The Office Action appears to assert that limitations of claim 5 requiring the second cryptosync to change between sessions presents a conflict with claim 1 which renders the limitations of claim 5 indefinite. Appellants respectfully disagree.

As is disclosed at p. 7, l. 7 –16 of the specification, according to at least one example embodiment, an LLCS may be incremented between communication sessions. Appellants respectfully submit, though this incrementing represents a change in the LLCS between communications sessions, as claim 5 recites, this incrementing does not represent the end of the life of LLCS, as the LLCS is only being incremented, not newly derived. Accordingly, Appellants respectfully

---

[27] *KSR Int'l Co. v. Telefax Inc.*, 127 S.Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007) (quoting *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006)).
[28] *See Oetiker*, 977 F. 2d at 1445, 24 USPQ2d at 1444.

submit there is no conflict between the limitations of claim 1 requiring the second cryptosync to have a life extending over multiple communications sessions and the limitations of claim 5 requiring the second cryptosync to change between communications sessions. Accordingly, Appellants respectfully submit the only assertion presented by the Examiner upon which the Examiner bases the conclusion that claim 5 is indefinite is incorrect. Consequently, Appellants respectfully submit claim 5 is not indefinite under §112, second paragraph, and there is no support in the Office Action for rejecting claim 5 under §112, second paragraph as being indefinite.

B. APPELLANTS SEEK THE BOARD'S REVIEW OF THE REJECTION OF CLAIMS 1, 4, 6, 7, 11 AND 12 UNDER 35 U.S.C. §103(A) AS BEING UNPATENTABLE OVER U.S. PATENT PUBLICATION 2005/0086468 TO MEANDZIJA ("MEANDZIJA") IN VIEW OF U.S. PATENT PUBLICATION 2004/0078334 TO MALCOLM ET AL. ("MALCOLM").

ARGUMENTS

In rejecting the above-referenced claims, the Office Action asserts the above-referenced claims are obvious in light of the combination of Meandzija and Malcolm. Appellants respectfully disagree with this assertion.

1. Brief Discussion of Meandzija and Malcolm

Meandzija discloses a user terminal of a wireless access network which can use a digital certificate to authenticate itself to access points of the wireless access network. In one embodiment, the user terminal includes a memory to store an identity certificate signed by a certificate that the user terminal can use for

authentication, where the identity certificate being based, at least in part, on hardware included in the user terminal. In one specific embodiment, the identity certificate is tied to the serial number of the user terminal.[29]

Malcolm discloses an information management system including one or more workstations each of which is connected to a network and includes an analyzer, which analyzes data sent from or received at the workstation. The analyzer uses policy data to determine an action to take with respect to the data. These actions can include extracting, checking, or storing digital certificates.[30]

2. The Office Action does not identify how each of the limitations of claim 1 are rendered obvious by the applied art.

First, Appellants respectfully submit the Office Action has not identified how each of the limitations of claim 1 is taught by the applied art. Appellants note, claim 1 recites "deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync, the first cryptosync having a life limited to the communication session, the communication session being defined as a period of time a channel for communication exists between the two communication devices, the second cryptosync having a life extending over multiple communication sessions". Accordingly, the limitations of claim 1 require a first cryptosync having a life limited to a communications session and a second cryptosync having life extending over multiple communications sessions. Appellants respectfully submit the Office Action has

[29] Meandzija, Abstract.
[30] Malcolm, Abstract.

not identified how the recited first and second cryptosyncs are taught or rendered obvious by any of the applied art, as is required to establish a *prima facie* case of obviousness.

With respect to the first cryptosync recited in claim 1, page 4 of the Office Action initially references a session certificate discussed in paragraph [0073] Meandzija. The Office Action identifies nothing in Meandzija as corresponding to the recited second cryptosync.

Further, the Office Action admits Meandzija fails to teach "deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync" as claim 1 recites. With respect to this limitation, the Office Action references Malcolm. With respect to the first and second cryptosyncs recited in claim 1, the Office Action references a digital certificate and a root certificate, from which the digital certificate may be derived, discussed in paragraph [0145] of Malcolm. Accordingly, Appellants assume the Office Action considers the digital certificate and root certificate of Malcolm as corresponding to the recited first and second cryptosync, respectively. However, Appellants respectfully submit the first and second cryptosyncs recited in claim 1 cannot be read upon the digital certificate and root certificate of Malcolm at least because nothing in Malcolm teaches limiting the derived digital certificate to a communication session while using a root certificate for multiple communications sessions as the limitations of claim 1 require of the recited first and second cryptosyncs, respectively. Specifically, the Examiner has identified nothing in Malcolm teaching the length of a life of either the root certificate or the derived certificate with respect to a communications session. Further, Malcolm appears

to be silent with respect to a lifespan of either the root or digital certificate. For at least this additional reason, Appellants respectfully submit the Office Action has not identified how each of the limitations of claim 1 are taught or rendered obvious by the applied art as is required to support a *prima facie* case of obviousness with respect to claim 1.

Next, Appellants respectfully submit even if, for the sake of argument, the teachings of Meandzija and Malcolm can be interpreted as covering each of the limitations of claim 1, *which Appellants specifically refute above*, the Office Action does not identify how the teachings of Malcolm and Meandzija can be combined or modified to result in a method including each of the limitations of claim 1.

Appellants note the Office Action's assertion on page 4 that it would be obvious to use Malcolm's information management system [with][31] Meandzija's digital certificate related to the user terminal hardware in a wireless network. However, the Office Action does not explain how one of ordinary skill in the art would combine or modify these systems in such a way that the limitations of claim 1 are taught. Specifically, Appellants respectfully submit if the systems of Meandzija and Malcolm are combined by being used simultaneously, the combined system would include the session certificate of Meandzija and the derived digital certificate of Malcolm, both of which the Office Action appears to identify as corresponding to the first cryptosync recited in claim 1. However, the Office Action does not assert that either of the session certificate of Meandzija and

[31] Appellants assume the word "with" was intended to be included in between the terms "system" and "Meandzija's" in line 22 on page 4 of the Office Action. Appellants' arguments are based on this assumption.

the derived digital certificate of Malcolm, alone, satisfy the requirements of the first cryptosync recited in claim 1. Accordingly, combining the systems of Meandzija and Malcolm by simply using the systems simultaneously, as the Office Action appears to suggest, would not teach the limitations of claim 1.

Appellants further note the Office Action includes **no arguments** asserting that it would be obvious to modify any of the session certificate taught by Meandzija, or the derived and root certificates taught by Malcolm to teach elements corresponding to either the first or second cryptosync recited in claim 1, nor does the Office Action provide a reasoning supporting the conclusion that such modification would be obvious.

Consequently, the Office Action provides no interpretation of the systems of Meandzija and Malcolm, alone or in combination, which teaches each of the limitations of claim 1. For at least this additional reason, Appellants respectfully submit the Office Action has not identified how each of the limitations of claim 1 are taught or rendered obvious by the applied art as is required to support a *prima facie* case of obviousness with respect to claim 1.

3. The Office Action does not articulate a reasoning having a rational underpinning supporting the legal conclusion of obviousness with respect to claim 1 as is required to support a rejection under §103.

Appellants respectfully submit, the Office Action does not identify sufficient motivation to combine Meandzija and Malcolm. As an initial matter, Appellants are aware that the teach-suggest-motivation rationale is not the only rationale

which can be used to support an obviousness rejection. However, some rationale is required.

With respect to the reasoning for combining the teachings of Meandzija and Malcolm, pages 4-5 of the Office Action states that it would be obvious to use the system of Malcolm with the system of Meandzija because it offers the advantage of ensuring that the transmission of data by their staff is always carried out securely, based on benefits discussed in paragraph [0028] of Malcolm.

Appellants respectfully submit, particularly in light of the Office Action's failure to articulate how one of ordinary skill in the art would combine or modify either of the systems of Meandzija and Malcolm to achieve a method teaching the limitations of claim 1, as is discussed above in section VII(B)(2) of this Brief, the Office Actions' statement regarding motivation to combine the teachings of Meandzija and Malcolm is conclusory and unsupported, and thus, cannot be used to support an obviousness rejection.[32]

Appellants respectfully submit the Office Action has identified nothing in Malcolm attributing the benefits discussed in paragraph [0028] of Malcolm specifically to the use of a root certificate and a digital certificate derived therefrom as discussed in paragraph [0145] of Malcolm. Further, a person of ordinary skill in the art would have no basis upon which to form a reasonable expectation that all possible combinations with, or modifications to, the system of Meandzija based on the teachings of Malcolm would succeed in achieving the benefits discussed in paragraph [0028] of Malcolm, as the Office Action suggests. Accordingly, assuming the teachings of Meandzija can be modified based on the

[32] *KSR Int'l Co. v. Telefax Inc.*, 127 S.Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007) (quoting *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006)).

teachings of Malcolm, or the that the teachings of Meandzija and Malcolm can be combined, neither of which Appellants admit, the Office Action has provided no support for the assertion that a person of ordinary skill in the art would view this unspecific[33] modification or combination as automatically resulting in achieving the advantages discussed in paragraph [0028] of Malcolm. Thus, Appellants respectfully submit, the Office Action does not identify a motivation to combine the teachings of Meandzija and Malcolm. Further, Appellants respectfully submit, the Office Action identifies no other rationale supporting the legal conclusion of obviousness.

Consequently, Appellants respectfully submit, the Office Action identifies no reasoning having a rational underpinning supporting the legal conclusion of obviousness as is required to support *prima facie* case of obviousness with respect to claim 1.

4. The Final Office Action does not establish a prima facie case of obviousness with respect to any of dependent claims 4, 6, 7, 11 and 12 as is required to support a rejection under §103.

Claims 4, 6, 11 and 12 depend from and thus incorporate the limitations of claim 1. The deficiencies of Meandzija and Malcolm with respect to claim 1 are discussed above. Accordingly, for at least the reasons discussed above with reference to claim 1, Appellants respectfully submit a *prima facie* case of obviousness has not been established with respect to claim 4.

[33] Point 8 on pages 4 and 5 of the Office Action appears to assert that it would be obvious to combine the systems of Meandzija and Malcolm or use them together, but does not specify how.

Further, for at least the following additional reasons, Appellants respectfully submit a *prima facie* case of obviousness has not been established with respect to any of claims 4, 6, 7, 11 and 12.

Claim 4

Claim 4 recites "wherein the second cryptosync is used for verifying message integrity by at least one of the two devices". The Examiner asserts this limitation is taught by paragraph [0007] of Meandzija. Paragraph [0007] discusses a digital certificate used by a user terminal to authenticate itself, as well as an identity certificate. As an initial matter, Appellants respectfully submit the recited second cryptosync cannot be read on either of the digital certificate and the identity certificate taught by paragraph [0007] of Meandzija. Specifically, the Office Action identifies nothing in Meandzija teaching that either the digital certificate or identity certificate of Meandzija 1) have a life extending over multiple communications sessions, or 2) are used to derive the value of the session certificate, which the Office Action identifies as corresponding to the recited first cryptosync[34]. Further, the Office Action provides no arguments stating that it would be obvious to modify either of the digital certificate and identity certificate of Meandzija to meet either of requirements 1) and 2) discussed above, both of which are required by claim 1 from which claim 4 depends. For at least these reasons, Appellants respectfully submit neither of the digital certificate and the identity certificate correspond to the recited second cryptosync. For this reason alone, Appellants respectfully submit the Office Action has not established that

[34] The Office Action at p. 4, lines 7-10.

any of the applied art, alone or in combination, teach or otherwise render obvious each of the limitations of claim 4 as is required to support a rejection under §103.

Further, the Office Action identifies nothing in Meandzija teaching the use of either the digital certificate or the identity certificate for verifying **message integrity** as claim 4 recites. For at least this additional reason alone, Appellants respectfully submit the Office Action has not established that any of the applied art, alone or in combination, teach or otherwise render obvious each of the limitations of claim 4 as is required to support a rejection under §103.

Claim 6

Claim 6 recites "wherein the deriving step derives the first cryptosync as at least a portion of the second cryptosync". With respect to this limitation, the Office Action references paragraph [0145] of Malcolm. However, the cited portion of Malcolm simply states that a digital certificate is derived from a root certificate. The cited portion of Malcolm is silent with respect to the particular manner in which the digital certificate is derived from the root certificate. Accordingly, the cited portion of Malcolm does not teach the first cryptosync being derived as ***at least a portion of*** the second cryptosync as the limitations of claim 6 require. Consequently, the Office Action does not identify how Malcolm, or any of the other applied art, alone or in combination, teaches or otherwise renders obvious each of the limitations of claim 6 as is required to support a rejection under §103.

Claim 7

Claim 7 recites "wherein the deriving step derives the first cryptosync as at least a portion of the second cryptosync and a fixed bit sequence". The Office Action asserts this limitation is taught by paragraph [0145] of Malcolm. As is stated above with reference to claim 4, the cited portion of Malcolm is silent with respect to a specific manner in which the digital certificate is derived from the root certificate. Further, paragraph [0145] appears to include no mention of a fixed bit sequence. Accordingly, the cited portion of Malcolm does not teach the first cryptosync being derived as ***at least a portion of*** the second cryptosync **and a fixed bit sequence** as the limitations of claim 7 require. Accordingly, the Office Action does not identify how Malcolm, or any of the other applied art, alone or in combination, teaches or otherwise renders obvious each of the limitations of claim 7 as is required to support a rejection under §103.

Claim 11

Claim 11 recites "wherein the deriving step derives a portion of the first cryptosync as the second cryptosync". The Office Action asserts this limitation is taught by paragraph [0145] of Malcolm. As is stated above with reference to claim 4, the cited portion of Malcolm is silent with respect to a specific manner in which the digital certificate is derived from the root certificate. Accordingly, the cited portion of Malcolm does not teach a portion of the first cryptosync being derived **as the second cryptosync** as the limitations of claim 11 require. Accordingly, the Office Action does not identify how Malcolm, or any of the other applied art, alone or in combination, teaches or otherwise renders obvious each of the limitations of claim 11 as is required to support a rejection under §103.

Claim 12

Claim 12 recites "wherein the deriving step derives a first portion of the first cryptosync as the second cryptosync and derives a second portion of the first cryptosync as a fixed bit sequence". The Office Action asserts this limitation is taught by paragraph [0145] of Malcolm. As is stated above with reference to claim 4, the cited portion of Malcolm is silent with respect to a specific manner in which the digital certificate is derived from the root certificate. Further, paragraph [0145] appears to include no mention of a fixed bit sequence. Accordingly, the cited portion of Malcolm does not teach a first portion of the first cryptosync being derived **as the second cryptosync** and a second portion being derived **as a fixed bit sequence** as the limitations of claim 12 require. Accordingly, the Office Action does not identify how Malcolm, or any of the other applied art, alone or in combination, teaches or otherwise renders obvious each of the limitations of claim 12 as is required to support a rejection under §103.

C. APPELLANTS SEEK THE BOARD'S REVIEW OF THE REJECTION OF CLAIMS 2 AND 3 UNDER 35 U.S.C. §103(A) AS BEING UNPATENTABLE OVER MEANDZIJA IN VIEW OF MALCOLM IN FURTHER VIEW OF U.S. PATENT PUBLICATION 2005/0172116 TO BURCH ET AL. ("BURCH").

ARGUMENTS

In rejecting the above-referenced claims, the Office Action asserts the above-referenced claims are obvious in light of the combination of Meandzija, Malcolm, and Burch. Appellants respectfully disagree with this assertion.

1. Brief Discussion of Burch

Burch discloses techniques for dynamically establishing and managing trust relationships. A first principal initially requests a community list. The community list includes identities of one or more second principals with which the first principal can establish trusted relationships with. The community list is associated with a trust specification. The trust specification defines the policies and access rights associated with interactions between the first principal and the second principals during any active trusted relationships. The first principal can dynamically subdivide, manage, and modify entries of the community list and the trust specification, assuming any such modifications are permissible according to global contracts and policies associated with the first principal.[35]

2. The Final Office Action does not establish a prima facie case of obviousness with respect to either of claims 2 and 3 as is required to support a rejection under §103.

Claims 2 and 3 depend from and thus incorporate the limitations of claim 1. The deficiencies of Meandzija and Malcolm with respect to claim 1 are discussed above. Burch does not remedy these deficiencies, neither does the Office Action rely on Burch to do so Accordingly, for at least the reasons discussed above with reference to claim 1, Appellants respectfully submit a *prima facie* case of obviousness has not been established with respect to either of claims 2 and 3.

[35] Burch, Abstract

Further, for at least the following additional reasons, Appellants respectfully submit a prima facie case of obviousness has not been established with respect to either of claims 2 and 3.

Claim 2

Claim 2 recites "wherein the second cryptosync is used for message encryption by at least one of the two devices". Page 6 of the Office Action admits the limitation is not taught by Meandzija. However, Page 6 of the Office Action asserts this limitation is taught by paragraph [0004] and [0023] of Burch. Paragraphs [0004] and [0023] of Burch teach using public keys for encrypting communications. Page 6 of the Office Action asserts that it would be obvious to use the teaching of Burch with those of Meandzija. However, the Office Action does not assert that it would be obvious to use the teachings of Burch with a cryptosync taught by Meandzija, or any other reference, which corresponds specifically with the recited second cryptosync. Specifically, even if it would be obvious to use a public key to encrypt a message in the system of Meandzija, *which Appellants do not admit,* the Office Action provides no arguments asserting that it would be obvious to encrypt a message specifically using a cryptosync that 1) has a life extending over multiple communications session or 2) is used to derive the value of the session certificate[36] of Meandzija. Both items 1) and 2) are required by claim 1 of the recited second cryptosync. Accordingly, the Office Action does not even assert that it would be obvious to use **the second**

[36] In rejecting claim 1, page 4 of the Office Action identifies the session certificate discussed in paragraph [0073] of Meandzija as corresponding to the recited first cryptosync.

cryptosync "for message encryption by at least one of the two devices" as the limitations of claim 2 require, nor does the Office Action provide any arguments supporting the legal conclusion that it would be obvious to do so, as is required to support a prima facie case of obviousness. Accordingly, the Office Action does not identify how Burch, or any of the other applied art, alone or in combination, teaches or otherwise renders obvious each of the limitations of claim 2 as is required to support a rejection under §103.

Claim 3

Claim 3 recites "wherein the second cryptosync is used for verifying message integrity by at least one of the two devices". In rejecting claim 3, the Examiner uses the same rationale used to reject claim 4 discussed above in section VII(B)(4) of this Brief. Accordingly, for the same reasons discussed above with respect to claim 4, Appellants respectfully submit the Office Action does not identify how any of the applied art, alone or in combination, teaches or otherwise renders obvious each of the limitations of claim 3 as is required to support a rejection under §103.

D. APPELLANTS SEEK THE BOARD'S REVIEW OF THE REJECTION OF CLAIM 5 UNDER 35 U.S.C. §103(A) AS BEING UNPATENTABLE OVER MEANDZIJA IN VIEW OF MALCOLM IN FURTHER VIEW OF U.S. PATENT PUBLICATION 2005/0177715 TO SOMIN ET AL. ("SOMIN").

ARGUMENTS

In rejecting the claim 5 the Office Action asserts claim 5 is obvious in light of the combination of Meandzija, Malcolm, and Somin. Appellants respectfully disagree with this assertion.

1. Brief Discussion of Somin

Somin discloses a system for organizing and storing information about multiple peer identities. New certificates are introduced that enable a user to efficiently create, modify, and delete identities and groups. New storage structures enable the user to list and search through existing identities, groups, and their related certificates. An identity certificate contains information about a peer identity. A group root certificate is created by a user when he decides to create a new group. When the group creator user wishes to invite another entity to join the group, it creates another type of certificate called a group membership certificate. The group membership certificate is logically "chained" to the group root certificate. The invitee checks the validity of these certificates by checking that the chaining has been properly done. The invitee may then be allowed to invite other entities to join the group by sending out its own group membership certificates.[37]

[37] Somin, Abstract.

2. The Final Office Action does not establish a prima facie case of obviousness with respect to claim 5 as is required to support a rejection under §103.

Claim 5 depends from and thus incorporates the limitations of claim 1. The deficiencies of Meandzija and Malcolm with respect to claim 1 are discussed above. Somin does not remedy these deficiencies, neither does the Office Action rely on Somin to do so Accordingly, for at least the reasons discussed above with reference to claim 1, Appellants respectfully submit a *prima facie* case of obviousness has not been established with respect to claim 5.

Further, for at least the following additional reasons, Appellants respectfully submit a prima facie case of obviousness has not been established with respect to either of claim 5.

Claim 5 recites "wherein the second cryptosync changes between communication sessions". Page 7 of the Office Action admits the Meandzija does not teach this limitation. Page 7 of the Office Action asserts paragraph [0043] of Somin teaches this limitation. Paragraph [0043] discusses a process whereby when a peer device 102 creates a new group, the peer device 102 creates a new group root certificate and a new group membership certificate. The Office Action appears to interpret the new group root certificate as corresponding to the recited second cryptosync. However, nothing in paragraph [0043] Somin or any other reference identified by the Office Action teaches a second cryptosync that **changes between communication sessions.** Specifically, the Office Action does not identify where Somin teaches the **creation** of a new group root certificate involving the **changing** of an existing group root certificate. Accordingly, even if for the sake of argument, the group root certificate of Somin corresponds to the

recited second cryptosync, *which Appellants do not admit*, the Office Action identifies nothing in Somin as teaching the **changing** of a group root certificate between communications sessions. Consequently, neither Somin, nor any of the other applied art, alone or in combination teaches "wherein the second cryptosync changes between communication sessions" as claim 5 recites. Thus, Appellants respectfully submit the Office Action does not identify how any of the applied art, alone or in combination, teaches or otherwise renders obvious each of the limitations of claim 5 as is required to support a rejection under §103.

E. APPELLANTS SEEK THE BOARD'S REVIEW OF THE REJECTION OF CLAIMS 8-10 AND 13-23 UNDER 35 U.S.C. §103(A) AS BEING UNPATENTABLE OVER MEANDZIJA IN VIEW OF MALCOLM IN FURTHER VIEW OF U.S. PATENT 6,980,658 TO REZAIIFAR ET AL. ("REZAIIFAR").

ARGUMENTS

In rejecting the above-referenced claims the Office Action asserts the above-referenced claims are obvious in light of the combination of Meandzija, Malcolm, and Rezaiifar. Appellants respectfully disagree with this assertion.

1. Brief Discussion of Rezaiifar.

Rezaiifar discloses a method and apparatus for encrypting transmission in a communication system. Transmission traffic is encrypted on separate protocol layers so that separate encryption elements can be assigned to separate types of transmission traffic. This allows implementation of different types of encryption

according to service requirements. Encryption elements use semi-permanent encryption keys with variable cryptosyncs.[38]

2. The Office Action does not establish a prima facie case of obviousness with respect to claim 8 as is required to support a rejection under §103.

Claim 8 depends from and thus incorporates the limitations of claim 1. The deficiencies of Meandzija and Malcolm with respect to claim 1 are discussed above. Rezaiifar does not remedy these deficiencies, nor the Examiner rely on Rezaiifar to do so. Accordingly, for at least the reasons discussed above with reference to claim 1, Appellants respectfully submit a *prima facie* case of obviousness has not been established with respect to claim 8.

Further, claim 8 recites "wherein the deriving step derives most significant bits of the first cryptosync as the portion of the second cryptosync and derives least significant bits of the first cryptosync as the fixed bit sequence". With respect to these limitations, the Office Action points to column 4, lines 46-62 of Rezaiifar. The cited portion of Rezaiifar discusses using an ENC-SEQ generator to provide a sequence number used to construct a crypto sync. Appellants assume the Office Action is interpreting the generated sequence as corresponding to the recited fixed bit sequence. However, the Office Action does not identify what in Rezaiifar is being interpreted as corresponding to the recited second cryptosync. Accordingly, the Office Action does not identify how the applied art, alone or in combination, teaches deriving a cryptosync having a portion of the second

[38] Rezaiifar, Abstract.

cryptosync **and** a fixed bit sequence, let alone specifically deriving "most significant bits of the first cryptosync as the portion of the second cryptosync" and specifically deriving "least significant bits of the first cryptosync as the fixed bit sequence", as claim 8 recites. Accordingly, the Office Action does not identify how Rezaiifar, or any of the other applied art, alone or in combination, teaches each of the limitations of claim 8 as is required to support a rejection under §103.

3. The Office Action does not establish a prima facie case of obviousness with respect to any of claims 9-10 and 13-23 as is required to support a rejection under §103.

First, Appellants note, for each of the rejections of claims 9-10 and 13-23, no reasoning is provided supporting the conclusion that it would be obvious to combine Meandzija, Malcolm and Rezaiifar in such a way that the limitations of the claim are taught. For at least this reason, Appellants respectfully submit a *prima facie* case of obviousness has not been established with respect to any of claims 9-10 and 13-23.

Next, Appellants note, the Office Action may intend to apply the same reasoning regarding obviousness discussed with respect to claim 8 to each of claims 9-10 and 13-23. However, if this is the case, Appellants respectfully submit, for each of the rejections of claims 9-10 and 13-23, there is no discussion in the Office Action regarding how the combination of the systems of Meandzija, Malcolm and Rezaiifar discussed with reference to the rejection of claim 8 would teach the limitations of any of claims 9-10 and 13-23. Further, there is no discussion in the Office Action regarding how any of the systems of Meandzija,

Malcolm and Rezaiifar would be further modified to teach the limitations of any of claims 9-10 and 13-23.

Accordingly, Appellants respectfully submit the Office Action has not identified how each of the limitations of any of claims 9-10 and 13-23 are taught or rendered obvious by the applied art as is required to support a *prima facie* case of obviousness with respect to claims 9-10 and 13-23.

Further, Appellants respectfully submit the Office Action does not identify how the following limitations are taught by the applied art.

Claim 9

Claim 9 recites "wherein the fixed bit sequence is a string of 0s". With respect to this limitation the Office Action references an EID value discussed in column 9, lines 11-22 of Rezaiifar. However, Appellants respectfully submit the EID bit 807 discussed in the portion of Rezaiifar referenced by the Office Action is a single bit, not a string of 0s. Further, the EID bit 807 is included in a frame 800 which is not taught by Rezaiifar as being a cryptosync as claim 9 requires. Accordingly, Appellants respectfully submit the Office Action does not identify how Rezaiifar, or any of the other applied art, alone or in combination, teaches or otherwise renders obvious each of the limitations of claim 9 as is required to support a rejection under §103.

Claim 10

Claim 10 recites "wherein the deriving step derives a 32 most significant bits of the first cryptosync as the second cryptosync and derives a 32 least

significant bits of the first cryptosync as a string of 0s". With respect to these limitations the Office Action again references an EID value discussed in column 9, lines 11-22 of Rezaiifar. However, as is discussed above, the EID bit 807 discussed in the portion of Rezaiifar referenced by the Office Action is a single bit, not a string of 32 0s. Further, the EID bit 807 is included in a frame 800 which is not taught by Rezaiifar as being a cryptosync. Accordingly, Appellants respectfully submit the Office Action does not identify how Rezaiifar, or any of the other applied art, alone or in combination, teaches or otherwise renders obvious each of the limitations of claim 10 as is required to support a rejection under §103.

Claim 13

Claim 13 recites "wherein the fixed bit sequence is a string of 0s". With respect to this limitation, the Office Action again identifies the EID value discussed in column 9, lines 11-22 of Rezaiifar. However, as is discussed above with respect to claim 10, the EID bit 807 discussed in the portion of Rezaiifar referenced by the Office Action is a single bit, not a string of 32 0s. Further, the EID bit 807 is included in a frame 800 which is not taught by Rezaiifar as being a cryptosync. Accordingly, Appellants respectfully submit the Office Action does not identify how Rezaiifar, or any of the other applied art, alone or in combination, teaches or otherwise renders obvious each of the limitations of claim 13 as is required to support a rejection under §103.

Claims 16 and 17

Claim 16 recites "wherein the deriving step is performed at a base station" and claim 17 recites "wherein the deriving step is performed at a mobile station". With respect to each of these limitations, the Office Action references column 3, lines 36-45 of Rezaiifar. The portion of Rezaiifar referenced by the Office Action discusses a CDMA wireless telephone system which generally includes mobile subscriber units 12 and base stations 14. Appellants assume the Office Action is identifying the mobile subscriber units 12 and base station 14 as corresponding to the base station recited in claim 16 and the mobile station recited in claim 17. However, there is no discussion of performing the operation of deriving a cryptosync at either the base station or the mobile station in the portion of Rezaiifar referenced by the Office Action. Accordingly, Appellants respectfully submit the Office Action does not identify how Rezaiifar, or any of the other applied art, alone or in combination, teaches or otherwise renders obvious each of the limitations of either claims 16 and 17 as is required to support a rejection under §103.

Claim 18

Claim 18 recites "encrypting a frame of information to send from the at least one of the two devices using the first cryptosync". With respect to this limitation the Office Action references column 2, lines 19-23 of Rezaiifar which discusses encrypting transmission traffic. However, there is no discussion in the Office Action of what in this portion of Rezaiifar is being considered as corresponding to the first cryptosync recited in claim 18, nor is there any

discussion of how any combination of Meandzija, Malcolm and Rezaiifar are being interpreted as teaching a first cryptosync meeting all the requirements of claim 1 which is used to encrypt a frame of information as the limitations of claim 18 require. Accordingly, Appellants respectfully submit the Office Action does not identify how Rezaiifar, or any of the other applied art, alone or in combination, teaches or otherwise renders obvious each of the limitations of claim 18 as is required to support a rejection under §103.

Claim 20

Claim 20 recites "incrementing the first cryptosync after the encrypting step". With respect to this limitation the Office Action references column 2, lines 38-48 of Rezaiifar, which teach incrementing a cryptosync value at a receiving end and a transmission end. However, claim 20 depends from claim 1 and the Office Action does not identify how Rezaiifar teaches the cryptosync mentioned in the passage of referred to by the Office Action being derived based on the value of a second cryptosync as claim 1 requires. Further, there is no discussion of how any of Meandzija, Malcolm and Rezaiifar are being modified or combined to teach incrementing a cryptosync value corresponding to the first cryptosync recited in claim 1 as the limitations of claim 20 require. Accordingly, Appellants respectfully submit the Office Action does not identify how Rezaiifar, or any of the other applied art, alone or in combination, teaches or otherwise renders obvious each of the limitations of claim 20 as is required to support a rejection under §103

Claim 21

Claim 21 recites "decrypting a frame of information received at the at least one of the two devices using the first cryptosync". With respect to this limitation the Office Action references column 5, lines 56-67 of Rezaiifar which decryption/encryption at a physical layer. However, there is no discussion of cryptosyncs in the portion of Rezaiifar referenced by the Office Action. Further, claim 21 depends from claim 1, and the Office Action does not identify where Rezaiifar teaches the encryption/decryption mentioned in the passage referred to by the Office Action being performed using a cryptosync derived based on the value of a second cryptosync as claim 1 requires of the recited first cryptosync. Additionally, there is no discussion of how any of Meandzija, Malcolm and Rezaiifar are being modified or combined to teach decrypting a frame of information received at the at least one of the two devices using a cryptosync value corresponding to the first cryptosync recited in claim 1, as the limitations of claim 21 require. Accordingly, Appellants respectfully submit the Office Action does not identify how Rezaiifar, or any of the other applied art, alone or in combination, teaches or otherwise renders obvious each of the limitations of claim 21 as is required to support a rejection under §103.

Claim 23

Claim 23 recites "incrementing the first cryptosync after the decrypting step". With respect to this limitation the Office Action references column 2, lines 38-48 of Rezaiifar which teach incrementing a crypto sync value at a receiving end and a transmission end. However, claim 23 depend from claim 1 and the Office

Action does not identify where Rezaiifar teaches the cryptosync mentioned in the passage referred to by the Office Action being derived based on the value of a second cryptosync as claim 1 requires. Further, there is no discussion of how any of Meandzija, Malcolm and Rezaiifar is being modified or combined to teach incrementing a cryptosync value corresponding to the first cryptosync recited in claim 1 as the limitations of claim 20 require. Accordingly, Appellants respectfully submit the Office Action does not identify how Rezaiifar, or any of the other applied art, alone or in combination, teaches or otherwise renders obvious each of the limitations of claim 23 as is required to support a rejection under §103.

F. APPELLANTS SEEK THE BOARD'S REVIEW OF THE REJECTION OF CLAIM 24 UNDER 35 U.S.C. §103(A) AS BEING UNPATENTABLE OVER MEANDZIJA IN VIEW OF MALCOLM IN FURTHER VIEW OF BURCH.

ARGUMENTS

In rejecting claim 24 the Office Action asserts claim 24 is obvious in light of the combination of Meandzija, Malcolm, and Burch. Appellants respectfully disagree with this assertion.

Claim 24 recites "deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync used to encrypt further communication between the two devices, the first cryptosync having a life limited to the communication session, the communication session being defined as a period of time a channel for communication exists between the two communication devices, the second cryptosync having a life extending over multiple communication sessions". Page

10 of the Office Action asserts the above-referenced limitations of claim 24 are taught by paragraph [0073] of Meandzija and paragraph [0145] of Malcolm. Further, for at least the same reasons discussed above in section VII(B)(2) of this Brief with respect to the rejection of claim 1, Appellants respectfully submit the Office Action has not identified how each of the above-referenced limitations of claim 24 are taught or rendered obvious by Meandzija and Malcolm. The Office Action does not apply Burch to teach the above-referenced limitations of claim 24. Accordingly, the Office Action has not identified how each of the limitations of claim 24 are taught or otherwise rendered obvious by the applied art, alone or in combination, as is required to support a *prima facie* case of obviousness with respect to claim 24.

Further, page 11 of the Office Action appears to cite the same motivation for combining the teachings of Meandzija and Malcolm used on page 4 of the Office Action in rejecting claim 1. Thus, for the same reasons discussed above in section VII(A)(3) of this Brief with respect to the rejection of claim 1, Appellants respectfully submit, the Office Action identifies no reasoning having a rational underpinning supporting the legal conclusion of obviousness with respect to claim 24 as is required to support a *prima facie* case of obviousness with respect to claim 24.

VIII. CONCLUSION.

In light of the foregoing arguments, Appellants respectfully request the Board to reverse the Final Office Action's rejections of claims 1-24.

The Commissioner is authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY & PIERCE, PLC

By _____ Reg. No. 64,371
for Gary D. Yacura, Reg. No. 35,416

GDY/JHA:eaf

P.O. Box 8910
Reston, VA 20195
(703) 668-8000

IX. CLAIMS APPENDIX.

Claims on Appeal:

1. (Previously Presented) A method of generating a cryptosync for a communication session between two communication devices, comprising:

deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync, the first cryptosync having a life limited to the communication session, the communication session being defined as a period of time a channel for communication exists between the two communication devices, the second cryptosync having a life extending over multiple communication sessions.

2. (Original) The method of claim 1, wherein the second cryptosync is used for message encryption by at least one of the two devices.

3. (Original) The method of claim 2, wherein the second cryptosync is used for verifying message integrity by at least one of the two devices.

4. (Original) The method of claim 1, wherein the second cryptosync is used for verifying message integrity by at least one of the two devices.

5. (Original) The method of claim 1, wherein the second cryptosync changes between communication sessions.

6. (Original) The method of claim 1, wherein the deriving step derives the first cryptosync as at least a portion of the second cryptosync.

7. (Original) The method of claim 6, wherein the deriving step derives the first cryptosync as at least a portion of the second cryptosync and a fixed bit sequence.

8. (Original) The method of claim 7, wherein the deriving step derives most significant bits of the first cryptosync as the portion of the second cryptosync and derives least significant bits of the first cryptosync as the fixed bit sequence.

9. (Original) The method of claim 8, wherein the fixed bit sequence is a string of 0s.

10. (Original) The method of claim 8, wherein the deriving step derives a 32 most significant bits of the first cryptosync as the second cryptosync and derives a 32 least significant bits of the first cryptosync as a string of 0s.

11. (Original) The method of claim 6, wherein the deriving step derives a portion of the first cryptosync as the second cryptosync.

12. (Original) The method of claim 11, wherein the deriving step derives a first portion of the first cryptosync as the second cryptosync and derives a second portion of the first cryptosync as a fixed bit sequence.

13. (Original) The method of claim 12, wherein the fixed bit sequence is a string of 0s.

14. (Original) The method of claim 1, wherein the deriving step comprises:

performing a pseudo-random function on the second cryptosync; and

generating the first cryptosync from output of the pseudo-random function.

15. (Original) The method of claim 14, wherein the generating step generates the first cryptosync as the output of the pseudo-random function.

16. (Original) The method of claim 1, wherein the deriving step is performed at a base station.

17. (Original) The method of claim 1, wherein the deriving step is performed at a mobile station.

18. (Original) The method of claim 1, further comprising:

encrypting a frame of information to send from the at least one of the two devices using the first cryptosync.

19. (Original) The method of claim 18, wherein the frame of information is a radio link protocol, RLP, frame.

20. (Original) The method of claim 18, further comprising:

incrementing the first cryptosync after the encrypting step.

21. (Original) The method of claim 1, further comprising:

decrypting a frame of information received at the at least one of the two devices using the first cryptosync.

22. (Original) The method of claim 21, wherein the frame of information is a radio link protocol, RLP, frame.

23. (Original) The method of claim 21, further comprising:

incrementing the first cryptosync after the decrypting step.

24. (Previously Presented) A method of generating a cryptosync for a communication session between two communication devices, comprising:

deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync used to encrypt further communication between the two devices, the first cryptosync having a life limited to the communication session, the communication session being defined as a period of time a channel for communication exists between the two

communication devices, the second cryptosync having a life extending over multiple communication sessions.

<End of Claims Listing>

X. EVIDENCE APPENDIX.

None.

XI. RELATED PROCEEDINGS APPENDIX.

None.